Oggier, Frédérique; **Belfiore, Jean-Claude**

On the secrecy gain of extremal even l-modular lattices. (English) Zbl 07136204

Exp. Math. 28, No. 4, 492-508 (2019).

Summary: The secrecy gain is a lattice invariant that appears in the context of wiretap lattice coding. It has been studied for unimodular lattices, for 2-, 3-, and 5-modular lattices. This paper studies the secrecy gain for extremal even l-modular lattices, for $l \in \{2, 3, 5, 6, 7, 11, 14, 15, 23\}$. We compute the highest secrecy gains as a function of the lattice dimension and the lattice level l. We show in particular that $l = 2, 3, 6, 7, 11$ are best for the respective ranges of dimensions $\{80, 76, 72\}$, $\{68, 64, 60, 56, 52, 48\}$, $\{44, 40, 36\}$, $\{34, 32, 30, 28, 26, 24, 22\}$, $\{18, 16, 14, 12, 10, 8\}$. This suggests that within a range of dimensions where different levels exist, the highest value of l tends to give the best secrecy gain. A lower bound computation on the maximal secrecy gain further shows that extremal lattices provide secrecy gains which are very close to this lower bound, thus confirming the good behavior of this class of lattices with respect to the secrecy gain.

MSC:

11H06 Lattices and convex bodies (number-theoretic aspects)

Keywords:

lattices; secrecy gain; theta series

Software:

SageMath

Full Text: DOI

References:

[1] Conway, [Conway And Sloane 99] J.; Sloane, N. J. A., Sphere Packings, Lattices and Groups (1999), New York: Springer, New York · Zbl 0915.52003

[2] Ernvall-Hytönen, [Ernvall-Hytönen 12] A.-M., On a Conjecture by Belfiore and Solé on Some Lattices, IEEE Trans. Inf. Theory, 58, 9, 5950-5955 (2012) · Zbl 1364.11132

[3] Ernvall-Hytönen, [Ernvall-Hytönen And Sethuraman 15] A.-M.; Sethuraman, B. A., Counterexample to the Generalized Belfiore-Solé Secrecy Function Conjecture for l-Modular Lattices (2015) · Zbl 1359.94591

[4] Hou, [Hou And Oggier 17] X.; Oggier, F., Modular Lattices from a Variation of Construction A over Number Fields, Adv. Math. Commun., 11, 4, 719-745 (2017) · Zbl 1439.11158

[5] Hou, [Hou Et Al. 14] X.; Lin, F.; Oggier, F., Construction and Secrecy Gain of a Family of 5-modular Lattices (2014)

[6] Lin, [Lin And Oggier 13] F.; Oggier, F., A Classification of Unimodular Lattice Wiretap Codes in Small Dimensions, IEEE Trans. Inf. Theory, 59, 6, 3295-3303 (2013) · Zbl 1364.94761

[7] Lin, [Lin And Oggier 12] F.; Oggier, F., Gaussian Wiretap Lattice Codes from Binary Self-dual Codes (2012)

[8] Lin, [Lin Et Al. 15] F.; Oggier, F.; Solé, P., 2- and 3-modular Lattice Wiretap Codes in Small Dimensions, Appl. Algeb. Eng. Commun. Comput., 25, 571, 571-590 (2015) · Zbl 1343.94098

[9] Nipp, [Nipp 91] G. L., Quaternary Quadratic Forms (1991), New York: Springer Verlag, New York · Zbl 0727.11018

[10] Oggier, [Oggier Et Al. 16] F.; Belfiore, J.-C.; Solé, P., Lattice Codes for the Wiretap Gaussian Channel: Construction and Analysis, IEEE Trans. Inform. Theory, 62, 10, 5690-5708 (2016) · Zbl 1359.94149

[11] Pinchak, [Pinchak 13] J., Wiretap Codes: Families of Lattices Satisfying the Belfiore-Solé Secrecy Function Conjecture (2013)

[12] Pinchak, [Pinchak And Sethuraman 14] J.; Sethuraman, B. A., The Belfiore-Solé Conjecture and a Certain Technique for Verifying it for a Given lattice (2014)

[13] Quebbemann, [Quebbemann 95] H.-G., Modular Lattices in Euclidean Spaces, J. Numb. Theory, 54, 190-202 (1995) · Zbl 0874.11038

[14] Quebbemann, [Quebbemann 97] H.-G., Atkin-Lehner Eigenforms and Strongly Modular Lattices, L'Enseign. Math., 43, 55-65 (1997) · Zbl 0898.11014

[15] Rains, [Rains And Sloane 98] E. M.; Sloane, N. J. A., The Shadow Theory of Modular and Unimodular Lattices., J. Numb. Theory, 73, 359-389 (1998) · Zbl 0917.11026

SageMath XXSageMath, The Sage Mathematics Software System (Version 7.3) (2016)

[16] Scharlau, [Scharlau And Schulze-Pillot 99] R.; Schulze-Pillot, R.; Matzat, B. H.; Greuel, Gm; Hiss, G., Algorithmic Algebra and Number Theory (Heidelberg, 1997), Extremal Lattices, 139-170 (1999), Berlin: Springer, Berlin

Gabriele Nebe and Neil Sloane XX